

2007

ANSA SSL Certificates and Encryption

Autonomic Software
October 2007



SSL Certificates and Encryption for ANSA

Autonomic Software houses a global update repository (GUR) of patches. This is the central location that the ANSA controller communicates with to retrieve patches and conduct registration of the software. Currently, all communication is processed HTTPS on Port 443. In the past, Autonomic Software used the standard and non-encrypted Port 80.

In previous editions of the ANSA UI and the controller config.xml file, the URL to communicate with the GUR was:

http:// 64.71.138.146 or http:// 64.71.138.146:81

Autonomic Software is now using secure socket layering (SSL) for communication between the ANSA UI and/or controller and the GUR. The URL is:

<https://www.autonomicsoftwaregur.com>

This URL will fall under the default port of 443. We do not need to specify the port number because we use the prefix of "https."

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL is included as part of both the Microsoft and Netscape browsers and most Web server products. Developed by Netscape, SSL also gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

The diagram below outlines an initiated SSL conversation between client and server. In this case, the client would be your controller and/or user interface. The server would be the GUR.

The server holds the SSL certificate. The client holds keys that enable it to be a trusted source to communicate with the server. The server knows what the keys are and will accept the encrypted keys from the client and compare to what the server has. Once the server compares keys and accepts the client keys, further communication is granted.



SSL Client



SSL Server

